PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-070566
(43)Date of publication of application : 10.03.1998

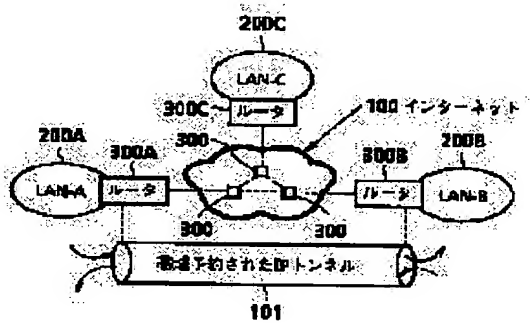
(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 12/66
H04L 29/08

(21)Application number : 08-227970
(22)Date of filing : 29.08.1996

(71)Applicant : KOKUSAI DENSHIN DENWA CO LTD <KDD>
(72)Inventor : MAEJIMA OSAMU
ITO YOSHIHIRO
ISHIKURA MASAMI
ASAMI TORU

(54) BAND SECURING TYPE VPN CONSTRUCTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To secure VPN(virtual private network) by the unit of a host or a sub-net.
SOLUTION: An IP tunnel 101 is constituted between routers 300A and 300B connected to internet 100 and a network resource reserving type protocol is started on this IP tunnel 101 to reserve the transmitting band width of the IP tunnel 101 to secure the band of VPN by the unit of the host to the sub-net. In addition, as the traffic control of routers 300A, 300 and 300B on the IP tunnel 101, the sending frequency of a packet which an inputting processor and an outputting processor within each router process is assigned by the ratio of a transmission band width reserved to the IP tunnel to simplify the algorithm of traffic control. In addition, each router 300A, 300 and 300B on the IP tunnel is provided with a reserving schedule function to manage the using time of band securing type VPN to secure a band at a designation date.



LEGAL STATUS

[Date of request for examination]	06.02.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3591996
[Date of registration]	03.09.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

10

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－７０５６６

(43)公開日　平成１０年（１９９８）３月１０日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 12/46			H04L 11/00	310	C
12/28		9744-5K	11/20		B
12/66			13/00	307	Z
29/08					

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）

(21)出願番号　特願平８－２２７９７０

(22)出願日　平成８年（１９９６）８月２９日

(71)出願人　０００００１２１４
国際電信電話株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　前島　治
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　伊藤　嘉浩
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　石倉　雅巳
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(74)代理人　弁理士　光石　俊郎　（外２名）

最終頁に続く

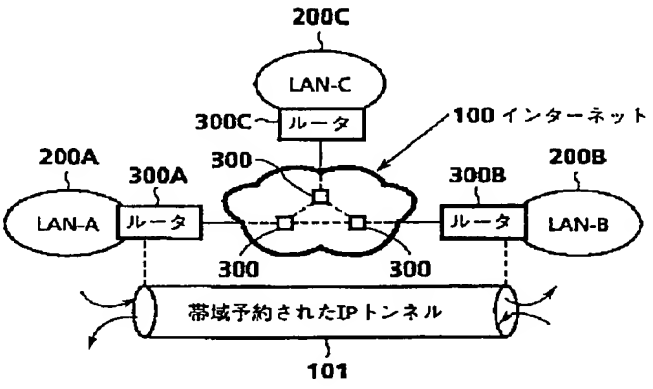
(54)【発明の名称】帯域確保型ＶＰＮ構築方法

(57)【要約】

【課題】　ＶＰＮの帯域をホスト或いはサブネット単位で確保すること。

【解決手段】　インターネット１００に接続されるルータ３００Ａ、３００Ｂ間にＩＰトンネル１０１を構成し、このＩＰトンネル１０１上に網資源予約型プロトコルを起動させて同ＩＰトンネル１０１の伝送帯域幅を予約することにより、ホスト或いはサブネット単位でＶＰＮの帯域確保を行う。また、ＩＰトンネル１０１上のルータ３００Ａ、３００、３００Ｂのトラヒック制御として、各ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、ＩＰトンネルに予約した伝送帯域幅の比で割り当てることにより、トラヒック制御のアルゴリズムを簡素化する。更に、ＩＰトンネル１０１上の各ルータ３００Ａ、３００、３００Ｂに予約スケジュール機能を持たせ、帯域確保型ＶＰＮの使用時間の管理を行うことにより、指定した日時での帯域確保を可能とする。

ネットワークモデル(実施例)



1

【特許請求の範囲】

【請求項１】　インターネットに接続されるルータ間にＩＰトンネルを構成し、このＩＰトンネル上に網資源予約型プロトコルを起動させることにより同ＩＰトンネルの伝送帯域幅の予約を行うことを特徴とする帯域確保型ＶＰＮ構築方法。

【請求項２】　ＩＰトンネル上のルータのトラヒック制御として、同ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、各ＩＰトンネルに予約した伝送帯域幅の比で割り当てることを特徴とする請求項１に記載の帯域確保型ＶＰＮ構築方法。

【請求項３】　ＩＰトンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型ＶＰＮの使用時間の管理を行うことを特徴とする請求項１または２に記載の帯域確保型ＶＰＮ構築方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はインターネット（Internet）上にＶＰＮ（Virtual Private Network(バーチャルプライベートネットワーク：仮想的専用網）の略記表示）を構築する方法に関し、特に、所望の伝送帯域幅の予約或いは確保をホスト単位或いはサブネット単位で可能にするものである。

【０００２】

【従来の技術】ＶＰＮとは、インターネット等の公衆網上で論理的なグループを構成し、且つ、そのグループ間で閉域性を保つ仕組みを設けたネットワークのことである。

【０００３】インターネット等の公衆網には、通常、不特定多数のユーザが接続している。そのため、基本的には特定のユーザだけの通信は出来ず、第三者による不正なアクセスが避けられないといったセキュリティ上の問題がある。

【０００４】そこで、近年、End-End（エンドーエンド）でセキュリティ対策を施すことによりインターネット上に仮想的に専用線を構築し、ＬＡＮ（Local Area Networkの略記表示）間接続の基幹回線として利用するＶＰＮ技術が注目されている。

【０００５】具体的には、従来のＶＰＮでは、エンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上で、特定の拠点間をインターネットを介して接続し、閉域性の有るグループを提供している。

【０００６】このようなＶＰＮを公衆網上に実現することにより、特定のユーザだけの通信が可能になり、インターネット等を仮想的な専用網として利用することができる。しかし、従来のＶＰＮはその仕様上、帯域等の網資源（ネットワークリソース）を保証していない。

【０００７】つまり、従来のＶＰＮは本来の専用線とは異なり、他のトラヒックの影響を受けて帯域幅が変動するため、通信特性を予測し難いといった問題がある。

2

【０００８】一方、QoS（Quality of Serviceの略記表示：帯域、遅延、揺らぎ等のサービス品質のこと）を重視した網資源予約型プロトコルであるＲＳＶＰ（Resource Reservation Protocol の略記）が提案されている。

【０００９】具体的には、図７に示すように、インターネット１００に接続される特定のＬＡＮ２００Ａと２００Ｂのホスト（端末）２０１全て、並びに、ＬＡＮ２００Ａと２００Ｂ間のルータ３００Ａ、３００及び３００Ｂ全てに、アプリケーション単位でＲＳＶＰをサポートさせている。図７中、記号ＲはＲＳＶＰのサポートを表す。

【００１０】そして、個々のアプリケーション毎にＲＳＶＰにより、特定のサービス品質を満たす網資源、例えば特定の帯域幅をネットワークに要求して予約し確保する。つまり従来は、エンドーエンドで、ＲＳＶＰによりアプリケーション単位に網資源を予約している。

【００１１】因みに、図８に示すように、ルータ３００Ａ、３００及び３００Ｂだけにアプリケーション単位でＲＳＶＰをサポートさせたとしても、両端のルータ３００Ａと３００Ｂで終端されてしまうため、ＲＳＶＰ上のアプリケーション２０２は双方のＬＡＮ２００Ａ、２００Ｂへは接続されない。

【００１２】さて、従来のＶＰＮにＲＳＶＰを組み合わせればＶＰＮの帯域を確保できるようにも思えるが、実際には、下記（１）、（２）の問題がある。

（１）従来は、ＲＳＶＰによりエンドーエンドで網資源（例えば帯域）を確保するので、ＶＰＮに接続した既存の全てのホストがＲＳＶＰをサポートしなければならない。

（２）現在のＶＰＮ利用方法の観点から見るとアプリケーション単位よりもホスト単位、サブネット単位の管理が望まれる場合も多く、そのような場合には、従来のアプリケーション単位での帯域確保は適さない。なお、サブネットとは、ＩＰアドレスのホスト部を更に分割（ネットワーク部とホスト部）して作成されたネットワークであり、図７や図８中でいえばＬＡＮ２００Ａ、２００Ｂを細分化したネットワークである。

【００１３】

【発明が解決しようとする課題】本発明は、上記問題点に鑑み、ホスト単位或いはサブネット単位で伝送帯域幅を確保することができる帯域確保型ＶＰＮを構築する方法を提供することを目的とする。

【００１４】

【課題を解決するための手段】上記課題を解決するため、本発明の帯域確保型ＶＰＮ構築方法は、インターネットに接続されるルータ間にＩＰトンネルを構成し、このＩＰトンネル上に網資源予約型プロトコルを起動させることにより同ＩＰトンネルの伝送帯域幅の予約を行うことを特徴とする。

3

【００１５】また、本発明の帯域確保型ＶＰＮ構築方法は、上記に加えて、ＩＰトンネル上のルータのトラヒック制御として、同ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、各ＩＰトンネルに予約した伝送帯域幅の比で割り当てることを特徴とする。

【００１６】更に、本発明の他の帯域確保型ＶＰＮ構築方法は、上記に加えて、ＩＰトンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型ＶＰＮの使用時間の管理を行うことを特徴とする。

【００１７】

【発明の実施の形態】

（発明の原理）次に、図９（ａ）（ｂ）と図１０を参照して、本発明に係る帯域確保型ＶＰＮ構築方法の原理を説明する。

【００１８】図９（ａ）に示す例では、インターネット１００に接続されるルータ３００Ａと３００Ｂ間にＩＰトンネル１０１を構成する。ここで、ＩＰとはインターネットプロトコル（Internet Protocol）の略記表示である。また、ＩＰトンネル１０１とは、周知の如く、ルータ３００Ａと３００Ｂ（ＩＰトンネル１０１の始点と終点）のＩＰアドレス等が記述されたＩＰヘッダを元のパケットに付加（カプセル化）することによって構成されるパケットが存在する区間である。終点のルータ例えば３００Ｂでは逆に、付加されたＩＰヘッダを外す。

【００１９】従って、両端のルータ３００Ａと３００Ｂがそれぞれ属するネットワーク（図９ではＬＡＮ）２００Ａ、２００Ｂ間のトラヒックを全てＩＰトンネル１０１に通すことにより、ＩＰトンネル１０１がＬＡＮ２００Ａ及び２００ＢにとってのＶＰＮとなる。

【００２０】このようなＩＰトンネル１０１上の各ルータ３００Ａ、３００及び３００ＢにＲＳＶＰ（網資源予約型プロトコル）をサポートさせ、ＩＰトンネル１０１上にＲＳＶＰを起動させる。この結果、ＲＳＶＰによる帯域確保はＩＰトンネル１０１即ちルータ間にて行われるため、双方のＬＡＮ２００Ａ、２００Ｂ上のアプリケーション２０２はＩＰトンネルの始点にてカプセル化され、ルータ３００Ａ～３００Ｂ間でＲＳＶＰ対応アプリケーションのデータとしてＩＰトンネル１０１上に確保された網資源（例えば帯域）を利用することが可能である。ここで、図９（ｂ）に示すように、ＩＰトンネル１０１区間はＲＳＶＰの帯域確保区間（本例ではルータ３００Ａ～３００Ｂ間）１０２を含む範囲にあれば良い。つまり、ＩＰトンネル１０１毎に伝送帯域幅の予約を行うことができる。また、伝送帯域幅の予約は従来のアプリケーション単位ではなく、各ＬＡＮ２００Ａと２００Ｂ上の各ホスト単位或いはサブネット単位で行われる。更に、各ホスト２０１はＲＳＶＰをサポートする必要がなくなる。

【００２１】また、伝送帯域幅の予約を解除するには、

4

ＩＰトンネル１０１の一端のルータ３００Ａ（または３００Ｂ）から他のルータ３００及び３００Ｂ（または３００及び３００Ａ）に対して、ＲＳＶＰプロトコルにより解除メッセージを送信すれば良い。

【００２２】このように、ＲＳＶＰプロトコル上で伝送帯域幅の確保が行われることから、各ノードのパラメータを手作業で変更する必要がなく、人的コストを削減でき、短期的な帯域需要に対して迅速且つ柔軟に帯域幅を割り当てることが可能である。また、帯域確保の解除も容易である。

【００２３】以上のように、ＩＰトンネル１０１と網資源予約型プロトコル（ＲＳＶＰ）を組み合わせることにより、他のトラヒックの影響を受けず、ホスト２０１単位またはサブネット単位の帯域確保が可能なＶＰＮを構築することができる。

【００２４】ところで、ＲＳＶＰは網資源の予約や確立を行うプロトコルであるが、ルータやホストにおけるQoS（帯域、遅延、揺らぎ等）を保証するための具体的な制御方法については、何も規定していない。従って、ネットワークにおけるQoS保証はルータやスイッチのトラヒック制御の実装に大きく依存する。パケットやスケジューリングのアルゴリズムとして報告されているＷＦＱ（Weighted Fair Queueing）等は、アプリケーションのトラヒック特性に応じて優先度を決定し帯域や遅延特性を制御するものであり、複雑なアルゴリズムである。

【００２５】本例では、ＩＰトンネル１０１毎に網資源パラメータとして伝送帯域幅のみを予約するので、帯域保証のための制御は、上記複雑なアルゴリズムではなく、図１０に示すような単純なパケットスケジューリングのアルゴリズムで対応可能である。特に、各ルータ３００Ａ、３００、３００Ｂ内部の入力プロセッサ及び出力プロセッサによって処理されるパケット数を、各ＩＰトンネル１０１に予約した伝送帯域幅の比で割り当てるというアルゴリズムを用いることにより、ＩＰトンネル１０１上の各ルータ３００Ａ、３００、３００Ｂのトラヒック制御が極めて簡素化する。

【００２６】図１０の場合は、パケットスケジューラ４０１と、＃１から＃ｎの複数のＲＳＶＰ用（ＩＰトンネル用）バッファ４０２と、非ＲＳＶＰ用バッファ４０３とでパケットスケジューリングを行う。即ち、隣接する任意のルータ間の帯域は複数のＩＰトンネルの分とそれ以外（非ＩＰトンネル）の分に区分されるので、ルータ内のバッファスペースも同様に、複数のＲＳＶＰ用バッファ４０２と、非ＲＳＶＰ用バッファ４０３に分ける。ＩＰトンネル内ではアプリケーションを特定する必要がないため、各ＲＳＶＰ用バッファ４０２に到着するパケットは同じトラヒック特性分布を有すると仮定する。そして、各ＲＳＶＰ用バッファ４０２のバッファサイズ及びパケットスケジューラ４０１による各ＲＳＶＰ用バッファ４０２からのパケット送出頻度を、各ＩＰトンネル

5

に予約した伝送帯域幅の比によって振り分けることで、アルゴリズムを簡素化する。

【００２７】なお、非ＲＳＶＰ用バッファ４０３からのパケット送出は、ＲＳＶＰ用バッファ４０２にパケットが無い場合に行う等、優先度を低くする。

【００２８】更に、本来ＲＳＶＰを用いた網資源の予約では、網資源を必要とする時にしか予約を行わないものである。しかし、ＩＰトンネル１０１上の各ルータ３００Ａ、３００、３００Ｂに予約スケジュール機能を持たせて帯域確保型ＶＰＮの使用時間の管理を行うことにより、従来のＲＳＶＰを拡張し、日時を指定して伝送帯域幅を予約することができる。

【００２９】（実施例）次に、図１～図６を参照して、本発明の実施例を説明する。図１は本発明を適用したネットワークモデルを示す。図２はルータ内部のトラヒック制御の構成例を示し、図３は図２の構成におけるトラヒック制御手順を示す。図４はトラヒック制御におけるパケットキューイングの説明図である。図５と図６はルータにおけるＶＰＮ予約スケジュールの処理手順（その１、その２）を示す。

【００３０】図１のネットワークモデルでは、インターネット１００に３個のＬＡＮ２００Ａ、２００Ｂ、２００ＣがＲＳＶＰをサポートしたルータ３００Ａ、３００Ｂ、３００Ｃを介して接続されている。インターネット１００のルータ３００もＲＳＶＰをサポートしている。そして、各２個のルータ３００Ａと３００Ｂ間、３００Ｂと３００Ｃ間、３００Ｃと３００Ａ間にそれぞれＩＰトンネル（図では１０１のみ示す）を設定し、ＬＡＮ２００Ａと２００Ｂ間のトラヒックは全てＩＰトンネル１０１を通し、ＬＡＮ２００Ｂと２００Ｃ間のトラヒックは全て該当するＩＰトンネル（図示省略）を通し、ＬＡＮ２００Ｃと２００Ａ間のトラヒックも全て該当するＩＰトンネル（図示省略）を通すようにしてある。

【００３１】このようなＩＰトンネル１０１の設定は、ＩＰトンネル両端のマシン（ＩＰトンネルサーバ）上にのみＩＰトンネル機能を付加することにより行われる。つまり、ＩＰトンネル一端のルータ例えば３００Ａが他端のルータ例えば３００Ｂに対してＩＰトンネルの設定を要求することにより行われる。前述のように、ＩＰトンネル始点（又は終点）によるＩＰパケットのカプセル化（又はカプセル解除）はＲＳＶＰによる帯域確保区間（図９の１０２参照）を含む範囲にて行われれば良いので、ＩＰトンネル機能の付加は伝送帯域の提供者（例えば通信事業者）が行う場合も考えられ、また、図９（ｂ）に示すように伝送帯域のユーザがＬＡＮ２００Ａ、２００Ｂ上にＩＰトンネルサーバ２０３で設定する場合もある。

【００３２】なお、本実施例では、各２個のＬＡＮ２００Ａと２００Ｂ間、２００Ｂと２００Ｃ間、２００Ｃと２００Ａ間を、従来のＶＰＮと同様、それぞれエンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上でインターネット１００を介して接続している。

6

【００３３】ルータ内部は、トラヒック制御のために、図２に示す構成としてある。一般に、ルータは入力側と出力側に複数のインターフェースを持つので、本実施例では、双方２つのインターフェースを持つものとして説明する。

【００３４】そこで、ルータ内部には、データ伝送に先立つ網資源予約型プロトコル（ＲＳＶＰ）による帯域確保の過程において、入力側にはＩＰトンネル数（予約数）と同数Ｎ個のＲＳＶＰ用入力バッファ３０１と、１個の非ＲＳＶＰ用（非予約型パケット用）入力バッファ３０２が作成される。また、出力側にはＩＰトンネル数（予約数）以上のＬ＋Ｍ個のＲＳＶＰ用出力バッファ３０３と、各出力インターフェース毎に１個の非ＲＳＶＰ用（非予約型パケット用）出力バッファ３０４が作成される。但し、各バッファ容量は各ＩＰトンネルに予約した伝送帯域幅に応じて可変であるものとしている。

【００３５】更に、ルータ内部には、入力用プロセッサ３０５及び各出力インターフェース毎の出力用プロセッサ３０６に加えて、予約識別用プロセッサ３０７と、これに連携する予約データベース３０８が設けられている。予約データベース３０８には、帯域予約の有無、各予約内容（送／受信側ＩＰアドレス、Ｐｏｒｔ（ポート）番号、プロトコルＩＤ、予約帯域幅等）の識別・照合・確認に必要なデータが格納される。図２中、３１１は元のパケット（ＩＰデータグラム）３０９にＩＰトンネル両端のルータのＩＰアドレス等が記述されたＩＰヘッダ３１０を付加（カプセル化）したパケットを示す。

【００３６】ＩＰトンネルに伝送帯域幅を予約するには、基本的には、ＬＡＮ上のホスト或いはサブネットが伝送帯域を必要とする時に、同ホスト或いはサブネットがＲＳＶＰ帯域確保区間の一端のルータに伝送帯域確保の要求を通知し、また、ＩＰトンネル上の送／受信側ＩＰアドレス、ポート番号、プロトコルＩＤ、予約帯域幅等の予約内容を通知する。同ルータはＲＳＶＰによりこれらの通知を次々に途中のルータ及びＩＰトンネル他端のルータに転送する。各ルータは帯域予約とその内容を予約データベース３０８に格納する。いずれかのルータで帯域確保が不可能であれば、ＲＳＶＰは帯域予約の要求を棄却する旨を始点のルータに通知する。

【００３７】次に、図２及び図３、図４を参照して、ルータにおけるトラヒック制御を説明すると、下記（１）～（５）のようになる。

【００３８】（１）図３のステップＳ１、Ｓ２のように、各入力インターフェースに到着したパケットに対し、予約識別用プロセッサ３０７がそれに連携する予約データベース３０８を参照して、帯域予約の有無、各予約内容（送／受信側ＩＰアドレス、ポート番号、プロト

コルＩＤ、予約帯域幅等）の識別・照合・確認を行う。

【００３９】（２）これら帯域予約の有無と各予約内容の識別等の後、予約識別用プロセッサ３０７はパケットを各々予約したＩＰトンネルに対応する入力バッファへ割り振る（図３のステップＳ３）。

【００４０】（３）入力プロセッサ３０５はパケット配信処理の際に、優先度の高い入力バッファからパケットを取り出す（図３のステップＳ４）。具体的には、図４を例に説明すると、下記①②のようになる。

①今、図４に示すように、ＲＳＶＰ用（帯域予約用）入力バッファ３０１が＃１、＃２，＃３の３個、非ＲＳＶＰ用（非予約型パケット用）入力バッファ３０２が１個有り、各ＩＰトンネルの予約帯域幅及び非予約型帯域幅の比がｉ：ｊ：ｋ：ｘであるとする。

②入力プロセッサ３０５は各帯域幅比に応じた頻度ｆ。で各入力バッファにアクセスして同バッファよりパケットを取り出す。具体的には、ｆ。＝ｍ／（ｉ＋ｊ＋ｋ＋ｘ）で表される頻度である。但し、ｍはｉ、ｊ，ｋ、ｘの何れかである。このようにしてＲＳＶＰ用入力バッファ＃１、＃２，＃３をアクセスした時、取り出すべきパケットがなければ、非ＲＳＶＰ用入力バッファ３０２内のパケットを、若しそこにパケットがあれば取り出す。

【００４１】（４）上記入力バッファからのパケット取出処理の後、入力プロセッサ３０５は、パケットを対応する出力バッファへ送る（図３のステップＳ５）。

【００４２】（５）その後、出力バッファ内のパケットを、各インターフェース毎に用意される出力プロセッサ３０６によって取り出し、ネットワークへ送出する（図３のステップＳ６とＳ７）。出力プロセッサ３０６が出力バッファ内のパケットを取り出す機能は、入力プロセッサ３０５を出力プロセッサ３０６と読み替え、入力バッファ＃１～＃３を出力バッファ＃１～＃３と読み替えるだけで上記（３）と同様であり、下記①②のようになる。

①今、図４に示すように、ＲＳＶＰ用（帯域予約用）出力バッファ３０３が＃１、＃２，＃３の３個、非ＲＳＶＰ用（非予約型パケット用）入力バッファ３０４が１個有り、各ＩＰトンネルの予約帯域幅及び非予約型帯域幅の比がｉ：ｊ：ｋ：ｘであるとする。

②出力プロセッサ３０６は各帯域幅比に応じた頻度ｆ。で各出力バッファにアクセスして同バッファよりパケットを取り出す。具体的には、ｆ。＝ｍ／（ｉ＋ｊ＋ｋ＋ｘ）で表される頻度である。但し、ｍはｉ、ｊ，ｋ、ｘの何れかである。このようにしてＲＳＶＰ用出力バッファ＃１、＃２，＃３をアクセスした時、取り出すべきパケットがなければ、非ＲＳＶＰ用出力バッファ３０４内のパケットを、若しそこにパケットがあれば取り出す。

【００４３】次に、図５と図６を参照して、ＶＰＮの予約スケジュール機能を説明する。前述の如く、ＲＳＶＰを用いた網資源予約では、本来、資源を必要とする時にしか伝送帯域の予約ができないが、本実施例では、下記（Ｉ）～（Ｖ）の処理により、指定した日時での伝送帯域の予約を可能にしている。なお、図５のステップＳ２８は図６のステップＳ２９に続く。

【００４４】（Ｉ）帯域確保型ＶＰＮ使用の事前予約が生じたら（図５のステップＳ２１）、ＲＳＶＰ（網資源予約型プロトコル）によりＩＰトンネル用の経路を設定可能かどうかを確認する（図５のステップＳ２２）。設定不可能であれば、事前予約を棄却する（図５のステップＳ２３、Ｓ２４）。

【００４５】（II）設定可能であれば、そのＩＰトンネル用経路上の全ルータ内の予約データベース（図２の３０８参照）を参照して、当該日時に要求するだけの伝送帯域幅を確保可能かどうか確認する（図５のステップＳ２３、Ｓ２５）。確保不可能であれば、事前予約を棄却する（図５のステップＳ２６、Ｓ２４）。

【００４６】（III）確保可能な場合は、ＩＰトンネル用経路上の全ルータ内の予約データベースに必要な予約情報（日時、予約帯域幅、送／受信側ＩＰアドレス、ポート番号、プロトコルＩＤ等）を登録する（図５のステップＳ２６、Ｓ２７）。

【００４７】（IV）指定日時になったら、下記①～②の処理をして、予約した伝送帯域幅の提供を開始する（図５のステップＳ２８～図６のステップＳ３１）。

①一定時間監視した後、予約者からのトラヒックが無いと判断される場合は、その事前予約を棄却する（図５のステップＳ２８、Ｓ２４）。

②事前予約されてないトラヒック（スケジュール外トラヒック）による帯域不足が生じる場合は、そのスケジュール外トラヒックの種別により以下（ａ）（ｂ）の処理でトラヒック抑制を行う（図６のステップＳ２９、Ｓ３０）。

（ａ）スケジュール外トラヒックが非ＲＳＶＰプロトコル（非網資源予約型プロトコル）の場合は、同トラヒックを全て棄却する。

（ｂ）スケジュール外トラヒックがＲＳＶＰプロトコルの場合は、それの利用者に予約解除の旨のメッセージを送出し、予約を解除する。

【００４８】（Ｖ）指定日時が経過したら、予約した伝送帯域幅の提供を終了する（図６のステップＳ３２）。

【００４９】

【発明の効果】本発明によれば、インターネットに接続されるルータ間にＩＰトンネルを構成し、このＩＰトンネル上に網資源予約型プロトコルを起動させることにより同ＩＰトンネルの伝送帯域幅の予約を行うので、他のトラヒックの影響を避けることができ、従来のＶＰＮよりも安定したトラヒック特性が得られる。また、網資源予約型プロトコルによる帯域確保がルータ間（ＩＰトンネル）にて行われるので、アプリケーション毎の網資源の予約が不要になり、ＬＡＮ上の個々のホスト或いはサ

9

ブネットは網資源予約型プロトコルをサポートしなくても良い。更に、帯域確保は網資源予約型プロトコルにより行われるので、帯域確保の設定及び解除が容易である。従って、各ノードのパラメータを手作業で変更する必要がなく、人的コストが削減できる。また、短期的な帯域需要に対して迅速且つ柔軟に伝送帯域幅を割り当てることができ、短期間の利用で大容量のデータ伝送が必要とされる場合に極めて有効である。

【００５０】また、本発明によれば、ＩＰトンネル上のルータのトラヒック制御として、同ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケット送出頻度を、各ＩＰトンネルに予約した伝送帯域幅の比で割り当てることにより、トラヒック制御のアルゴリズムが極めて簡素化する。

【００５１】更に、本発明によれば、ＩＰトンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型ＶＰＮの使用時間の管理を行うことにより、網資源予約型プロトコルを用いた予約では本来網資源を必要とする時にしか予約できないものが、将来の指定した日時での伝送帯域幅を確保することができる。

【図面の簡単な説明】

【図１】本発明を適用したネットワークモデルを示す図。

【図２】ルータ内部のトラヒック制御の構成例を示す図。

【図３】図２の構成におけるトラヒック制御手順を示す図。

【図４】トラヒック制御におけるパケットキューイングの説明図。

【図５】ルータにおけるＶＰＮ予約スケジュールの処理手順（その１）を示す図。

10

【図６】ルータにおけるＶＰＮ予約スケジュールの処理手順（その２）を示す図。

【図７】従来のＲＳＶＰを示す図。

【図８】ＬＡＮのホストがＲＳＶＰをサポートしない場合の従来のＲＳＶＰの欠点を示す図。

【図９】本発明の原理を示す図。

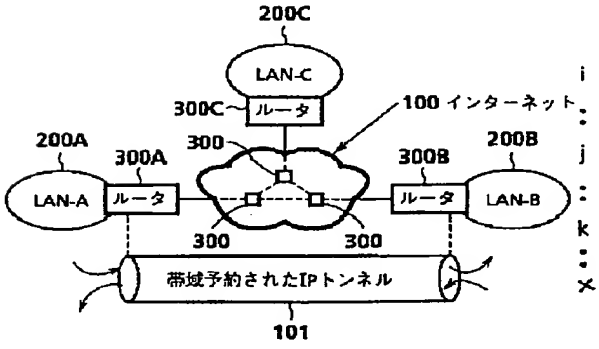
【図１０】パケットスケジューリングのアルゴリズム簡素化の説明図。

【符号の説明】

１００　インターネット
１０１　ＩＰトンネル
１０２　ＲＳＶＰによる帯域確保区間
２００Ａ、２００Ｂ、２００Ｃ　ＬＡＮ
２０１　ホスト
２０２　アプリケーション
２０３　ＩＰトンネルサーバ
３００Ａ、３００Ｂ、３００Ｃ、３００　ルータ
３０１　ＲＳＶＰ用入力バッファ
３０２　非ＲＳＶＰ用入力バッファ
３０３　ＲＳＶＰ用出力バッファ
３０４　非ＲＳＶＰ用出力バッファ
３０５　入力プロセッサ
３０６　出力プロセッサ
３０７　予約識別用プロセッサ
３０８　予約データベース
３０９　ＩＰデータグラム
３１０　ＩＰヘッダ
４０１　パケットスケジューラ
４０２　ＲＳＶＰ用（ＩＰトンネル用）バッファ
４０３　非ＲＳＶＰ用バッファ

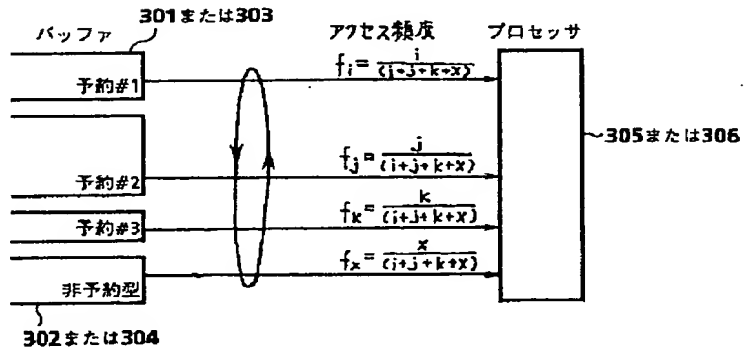
【図１】

ネットワークモデル(実施例)



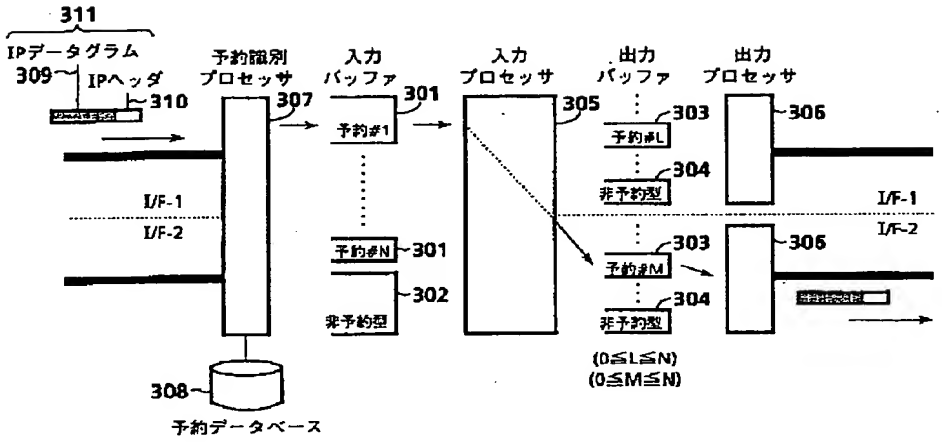
【図４】

パケットキューイング



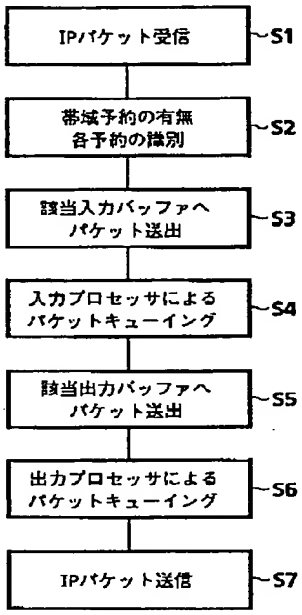
【図２】

ルータでのトラヒック制御



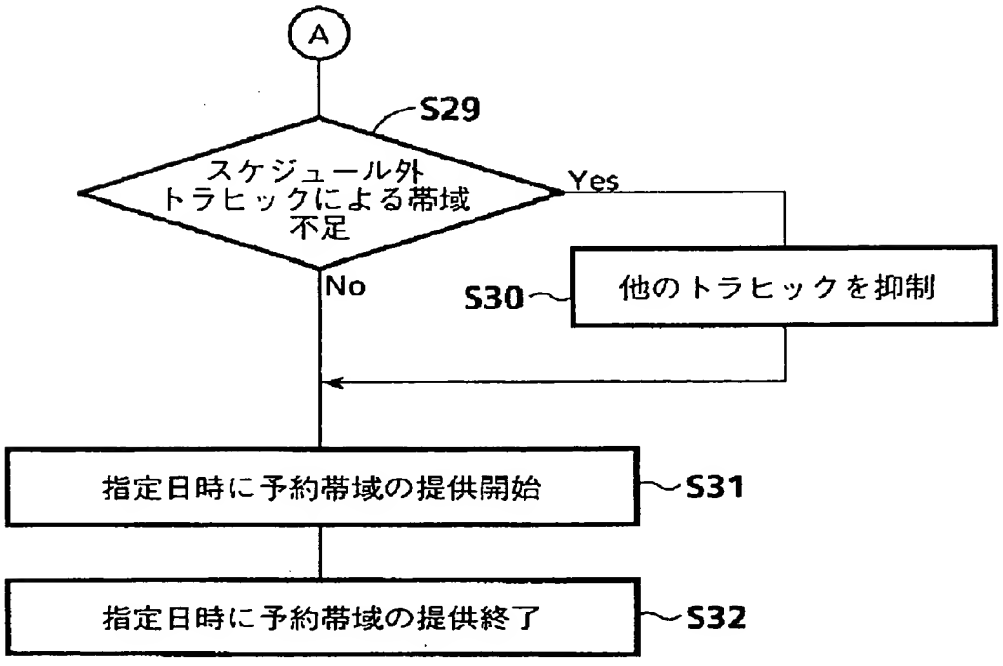
【図３】

実施例(ルータにおけるトラヒック制御)



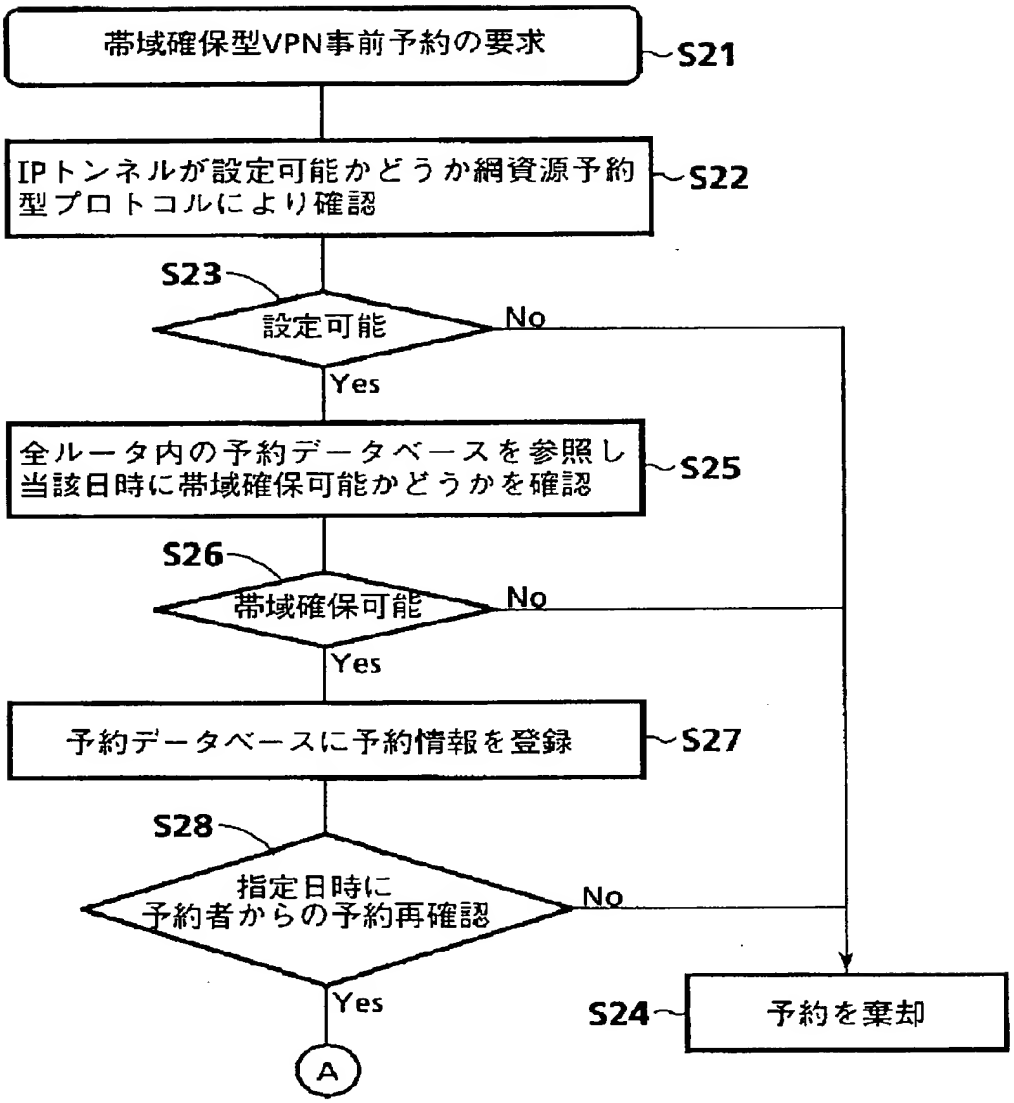
【図６】

VPNの予約スケジュール機能(その2)



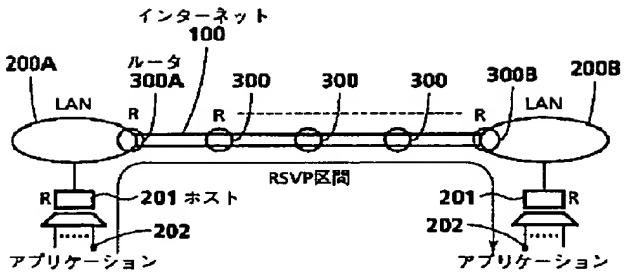
【図５】

VPNの予約スケジュール機能(その1)



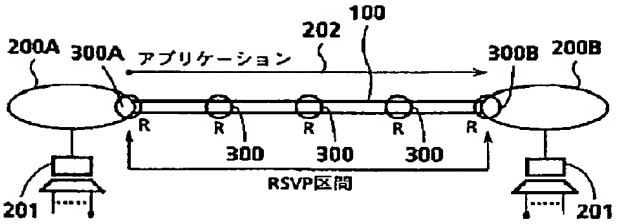
【図７】

従来のRSVP



【図８】

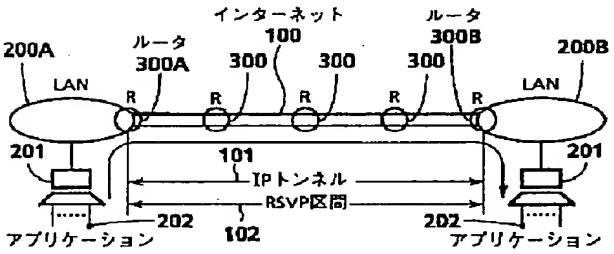
従　来



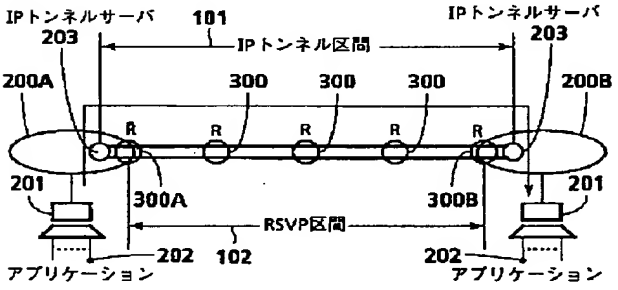
【図９】

発　明　(原　理)

(a)

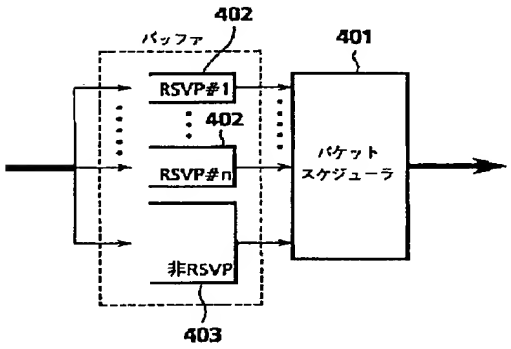


(b)



【図１０】

発明(パケットスケジューリング)



フロントページの続き

(72)発明者　浅見　徹
東京都新宿区西新宿二丁目３番２号　国際
電信電話株式会社内